CLAIMS

1. A data processing method performed by a first processing device and a second processing device when the first data processing device holds first authentication key data and encryption key data and the second data processing device holds second authentication data corresponding to the first authentication data and decryption key data corresponding to the encryption data, comprising:

a first step by which the first data processing device uses the first authentication key data and the second processing device uses the second authentication key data, and authentication is performed between the first data processing device and the second data processing device;

a second step by which when the second data processing device verifies the first data processing device by the authentication in the first step, the first processing device uses the encryption key data for encryption and decrypts encrypted data provided to the second data processing device by using the decryption key data, and

a third step by which when the second data processing device judges that decryption data obtained by the decryption in the second step is decrypted adequately, the second data processing device uses the decryption data as the data is effective.

2. A data processing method as set forth in claim 1, wherein

in the first step, the first data processing device and the second data processing device perform encryption and decryption of predetermined data based on a first encryption algorithm and a first decryption algorithm corresponding to the first encryption algorithm and perform the authentication, and

in the second step, the second data processing device decrypts the encrypted data encrypted based on a second encryption algorithm based on a second decryption algorithm corresponding to the second encryption algorithm.

3. A data processing method as set forth in claim 1, wherein the first data processing device is verified in the second step, when the second data processing device judges that the first authentication key data and the second authentication data are the same by the authentication in the first step.

4. A data processing method as set forth in claim 1, wherein, when the first authentication key data

is generated by a predetermined generation method by using predetermined key data, the first step comprises:

a fourth step by which the first data processing device provides key designation data designating key data used for generation of the first authentication key data to the second data processing device,

a fifth step by which the second data processing device generates the second authentication key data by a predetermined generation method by using the key data designated by the key designation data received -in the fourth step,

a sixth step by which the first data processing device uses the first authentication key data and uses the second authentication key data generated by the second data processing device in the fifth step to perform the authentication, and

a seventh step by which when the second data processing device judges that the first authentication data and the second authentication data are the same, the first data processing device is verified.

5. A data processing system comprising:

a first data processing device holding first authentication key data and encryption key data, and a second data processing device holding second authentication key data corresponding to the first authentication key data, and decryption key data corresponding to the encryption key data, wherein

the first data processing device uses the first authentication key data and the second data processing device uses the second authentication key data, and the authentication is performed between the first data processing device and the second data processing device,

the second data processing device decrypts encrypted data provided to the second data processing device by the first data processing device by using the encryption key data for encryption by using the decryption data, when the second data processing device verifies the first data processing device by the authentication, and

the second data processing device uses the decryption data as the data is effective, when the second data processing device judged decryption data obtained the decryption is decrypted adequately.

6. A data processing method performed by a data processing device holding authentication key data and encryption key data, comprising:

a first step of performing authentication with an authenticated side by using the authentication key data,

a second step of encrypting predetermined data by using the encryption key data after the authentication in the first step, and

a third step of outputting data obtained the encryption in the second step to the authenticated side.

7. A data processing method as set forth in claim 6, wherein when authenticating means of said authenticated side holding key data uses the key data designated from the data processing device holding the first authentication key data, generates second authentication key data based on predetermines generation method, performs authentication with the data processing device by using the second authentication key data and uses the data outputted in the third step as the data is effective, conditional on confirming that the first authentication key data and the second authentication key data are the same,

the first step comprises:

a fourth step of providing key designation data designating the key data used when the first authentication key data is generated based on the predetermined generation method to the authenticating means, and

a fifth step of performing the authentication with the authenticating means by using the first authentication key data.

8. A data processing device encrypting predetermined data and outputting the data to an authenticated side, comprising:

storing means for storing authentication key data and encryption key data;

authenticating means for performing authentication with an authenticated side by using the authentication key data;

encryption means for encrypting predetermined data by using the encryption key data after the authentication of the authenticating means, and

output means for outputting data obtained by the encryption of the encryption means to the authenticated side.

9. A program executed by a data processing device holding authentication key data and encryption key data, comprising:

a first step of performing authentication with an authenticated side by using the authentication key data;

a second step of encrypting predetermined data by using the encryption key data after the authentication in the first step, and

a third step of outputting data obtained by the encryption in the second step to the authenticated side.

10. A data processing method performed by a data processing device holding authentication key data and decryption key data, comprising:

a first step of performing authentication with means to be authenticated by using the authentication key data;

a second step of decrypting data received from the means to be authenticated by using the decryption key data, and

a third step of using data obtained by the decryption in the second step as the data is effective, when verifying the means to be authenticated by the authentication in the first step.

11. A data processing method as set forth in claim 10, wherein when the data processing device holding predetermined key data performs authentication with the means to be authenticated holding first authentication

key data generated by predetermined generation method by using the key data and hard to restore the key data,

the first step comprises:

a fourth step of receiving key designation data designating the key data from the means to be authenticated,

a fifth step of generating second authentication key data by a predetermined generation method by using the key data designated by the key designation data received in the fourth step,

a sixth step of performing the authentication with the means to be authenticated using the first authentication key data for the authentication by using the second authentication key data generated in the fifth step, and

a seventh step of verifying the means to be authenticated when judging that the first authentication use data and the second authentication use data by the authentication are the same in the sixth step.

12. A data processing method as set forth in claim 10, wherein, a function of a data processing device permitted by the means to be authenticated related to the key data, or an access to data held by the data processing device is executed in the third step.

13. A data processing device holding authentication key data and decryption key data, comprising:

authenticating means for authenticating with means to be authenticated by using the authentication key data;

input means for inputting data from the decryption key data;

decryption means for decrypting the data inputted from the means to be authenticated via the input means by using the decryption key data, and

control means for using data obtained by the decryption of the decryption means as the data is effective when the means to be authenticated is verified by the authentication of the authenticating means.

14. A program executed by a data processing device holding authentication key data and decryption key data, comprising:

a first step of performing authentication with means to be authenticated by using the authentication key data;

a second step of decrypting data received from the means to be authenticated by using the decryption key data, and a third step of using data obtained by the decryption in the second step as the data is effective when the means to be authenticated is verified by the authentication in the first step.